photonics

IMPACT FACTOR 2.1

CITESCORE 2.6

Article

Hands-On Quantum Cryptography: Experimentation with the B92 Protocol Using Pulsed Lasers

Sara P. Gandelman, Alona Maslennikov and Georgi Gary Rozenman

Special Issue

Quantum Optics: From Fundamental Research to Technological Applications

Edited by

Dr. Georgi Gary Rozenman and Dr. Satyendra Mishra

MDPI

https://doi.org/10.3390/photonics12030220

photonics

MDPI

Article

Hands-On Quantum Cryptography: Experimentation with the B92 Protocol Using Pulsed Lasers

Sara P. Gandelman [1], Alona Maslennikov [2] and Georgi Gary Rozenman [3,*]

[1] The Raymond and Beverly Sackler School of Physics and Astronomy, Tel Aviv University, Tel Aviv 69978, Israel; sarag@mail.tau.ac.il
[2] Department of Chemistry, Boston University, Boston, MA 02215, USA; alonam@bu.edu
[3] Research Laboratory of Electronics, MIT-Harvard Center for Ultracold Atoms, Department of Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
* Correspondence: gary95@mit.edu

Abstract: Quantum cryptography continues to be an area of significant research and educational interest. Here, a straightforward and reliable approach to both the experimental and theoretical aspects of quantum key distribution is presented, tailored for senior undergraduate students. Focusing on illustrating the essential concepts of the B92 protocol through a combination of optical experiments and custom-developed computational tools, this work offers a thorough exploration of quantum cryptography according to the principles of the B92 protocol.

Keywords: quantum; key; distribution; cryptography

Received: 26 January 2025
Revised: 19 February 2025
Accepted: 21 February 2025
Published: 28 February 2025

Citation: Gandelman, S.P.; Maslennikov, A.; Rozenman, G.G. Hands-On Quantum Cryptography: Experimentation with the B92 Protocol Using Pulsed Lasers. *Photonics* **2025**, *12*, 220. https://doi.org/10.3390/photonics12030220

1. Introduction

Today, ensuring the privacy of communication is more critical than ever, driving the need for secure message transmission methods [1]. Quantum key distribution (QKD) has become a leading approach for achieving secure communication, exploiting quantum mechanical properties to protect information from potential eavesdroppers [2–4]. The B92 protocol [5,6] provides an efficient method for distributing cryptographic keys using non-orthogonal quantum states, ensuring high levels of security against interception. Unlike classical cryptographic techniques, in which security depends on computational limitations, quantum cryptography leverages fundamental physical principles for inherent protection [7].

Historically, cryptography focused on transforming messages into coded formats that could not be interpreted without a key, providing secrecy even if intercepted [8]. However, classical encryption schemes, including those based on complex algorithms or key exchange methods (e.g., Diffie–Hellman), face increasing vulnerabilities as computational abilities advance and quantum computing becomes feasible [9]. Quantum computers, with their ability to solve mathematical problems, such as factorization, far more efficiently than classical computers, pose a significant threat to traditional cryptography, necessitating new solutions like QKD that are fundamentally secure [10].

A fundamental principle of quantum mechanics is that any measurement of a quantum state inevitably disturbs it—a concept known as measurement-induced disturbance [11]. Combined with the no-cloning theorem, which states that an unknown quantum state cannot be perfectly copied, this principle forms the foundation of quantum key distribution (QKD) security.

The B92 protocol utilizes only two non-orthogonal quantum states to establish a shared secret key, ensuring that any eavesdropping attempt introduces detectable disturbances [6]. Although initially proposed over 30 years ago, B92 continues to be explored in various experimental implementations [12,13] and remains a strong candidate for robust and secure QKD channels. Its simplicity and effectiveness make it particularly suitable for both theoretical investigations and practical applications in modern quantum communication [14]. Beyond its fundamental role in quantum cryptographic protocols, QKD serves as a versatile testbed for exploring various physical phenomena. It has been utilized in studies involving plasmonic nanoparticles, as well as in the advancement of single-photon detectors [15,16]. For instance, recent research has demonstrated how photonic encryption can be achieved using optical activity and third-order nonlinearities in Kerr-like nanofluids functionalized with plasmonic nanoparticles [15]. These systems exploit polarization rotation and nonlinear optical effects to implement XOR logic gates, offering a classical parallel to quantum information processing techniques. Such developments highlight the broader applicability of QKD-inspired methods beyond standard quantum optics, demonstrating their relevance in areas ranging from nanophotonics to advanced materials science.

With the rapid growth in the demand for educational quantum experiments in recent years [17–22] the implementation of a true B92 QKD system presents several practical challenges that must be addressed to realize its full potential in real-world applications. Such challenges include the requirements for single-photon sources, precise detection equipment, and a low-noise environment—all of which can be costly and technically demanding. These limitations make widespread adoption difficult, particularly in educational settings [23]. To address these challenges, pulsed lasers can be used as classical light sources to provide a more accessible emulation of the B92 protocol. Although such emulation lacks the absolute security of a true single-photon system, it offers an excellent way to explore the fundamental concepts of QKD in a practical setting.

In this work, we present an educational experiment that demonstrates the B92 quantum cryptography protocol without the need for specialized equipment, such as single-photon sources. Instead, the use of pulsed lasers allows for an accessible approximation of the protocol, which can be conducted in a standard undergraduate laboratory. While this emulation does not achieve true quantum security—since genuine protection requires that each information bit is conveyed by a single photon—it provides valuable insights into QKD fundamentals, particularly the detection of eavesdropping attempts. This setup also illustrates the significance of the no-cloning theorem and the role of measurement disturbances in securing quantum communications.

The objective of this work is to simplify the experimental setup for the B92 protocol to enhance its accessibility while retaining its educational value. By using standard optical components, such as pulsed lasers, polarizers, and detectors, students gain hands-on experience in the use of non-orthogonal quantum states for secure key transmission and the detection of eavesdropping, even within the constraints of classical emulation.

2. B92 Protocol with Alice and Bob

The B92 protocol is a QKD scheme that relies on the principles of quantum mechanics to provide secure communication between two parties, traditionally known as Alice (the sender) and Bob (the receiver). Unlike the BB84 protocol, the B92 protocol uses only two non-orthogonal states, simplifying the state preparation process while ensuring secure key distribution.

2.1. Protocol Overview

In the B92 protocol, Alice randomly generates a sequence of classical bits (0 or 1) and encodes each bit into one of two non-orthogonal quantum states. In our implementation:

- Bit value **0** is represented in the **+ basis** at **0°**.
- Bit value **1** is represented in the **x basis** at **45°**.

Then, Alice sends the quantum states to Bob, who measures them on a randomly chosen basis:

- The **+ basis** (0° or 90°) or
- The **x basis** (45° or −45°).

The probabilities associated with Bob's measurements are as follows:

- If Alice sends **0 in basis +**, Bob has:
  - A **50%** probability of measuring **0 in basis +**,
  - A **25%** probability of measuring **1 in basis x**,
  - A **25%** probability of measuring **0 in basis x**.
- If Alice sends **1 in basis x**, Bob has:
  - A **50%** probability of measuring **1 in basis x**,
  - A **25%** probability of measuring **0 in basis +**,
  - A **25%** probability of measuring **1 in basis +**.

2.2. Measurement Outcomes and Grant/Deny Criteria

Bob applies a "grant or deny" condition based on the measurement outcomes to determine whether the measured bit should be included in the final key:

- If Bob measures **0 in basis x** or **1 in basis +**, he **grants** the bit.
- Otherwise, he **denies** the bit.

The "granted" bits are those that are retained for further key processing, whereas the "denied" bits are discarded. This selection ensures that Bob only keeps results that are consistent with Alice's original encoding under quantum mechanical principles.

2.3. Experimental Perspective

In an experimental setup, Alice's quantum states can be prepared using polarized photons or other quantum systems capable of encoding qubit information. Bob's measurement basis is typically selected using a polarizer or similar device, followed by a detector that counts the number of photons. The experimental outcomes align with the theoretical probabilities when Bob measures the received quantum state. The randomness introduced by both Alice and Bob in their choices ensures that any potential eavesdropper cannot predict the outcome without being detected, providing key security.

2.4. Experimental Perspective

To further ensure the integrity of the experimental implementation, the state preparation and detection processes must be carefully calibrated. The choice of polarization states directly impacts the accuracy of the measurements. In this work, we utilize a pulsed laser source with a well-defined polarization state to mimic single-photon sources while maintaining an affordable and accessible setup. Bob's detection process relies on a PBS to separate the photon states into distinguishable paths, with each path leading to a dedicated detector. The detection results are recorded and analyzed using a computational script that maps the measurement outcomes to key bits. Additionally, practical considerations such as optical misalignment, detector inefficiencies, and environmental noise must be accounted

for. These factors introduce experimental uncertainties, which we mitigate through repeated measurements and statistical averaging. The data acquisition process is further refined by implementing post-selection criteria, ensuring that only valid measurements contribute to the final key. This experimental approach provides an accessible yet robust demonstration of the B92 protocol, making it a valuable tool for educational purposes. The setup highlights the fundamental principles of quantum cryptography while balancing affordability and feasibility in a laboratory setting.

3. The Experimental Apparatus

In the experimental setup, Alice uses a pulsed laser source to generate light polarized in two distinct, non-orthogonal directions, corresponding to the states used in the B92 protocol. A polarizer and half-wave plate (HWP) adjust the polarization of the incident light to the appropriate non-orthogonal state for key distribution. While this setup emulates a single-photon source, enabling Alice to transmit information securely, it does not achieve the true single-photon level necessary for absolute quantum security. Bob's apparatus consists of a half-wave plate, a polarizing beam splitter (PBS), and two detectors. He randomly selects its measurement basis by rotating the polarization plate and then uses the PBS and detectors to determine whether the incoming light was transmitted or reflected, thereby identifying the bit sent by Alice.

The apparatus is designed to emulate the behavior of a true quantum key distribution system but uses classical optical components such as pulsed lasers, making it accessible for educational laboratories. In the B92 protocol, Eve's presence as an eavesdropper can be detected if she attempts to measure the polarization of the transmitted photon, as her actions will inevitably disturb the system and introduce detectable errors. This experimental setup effectively demonstrates the basic principles of B92 quantum cryptography, including the security benefits derived from the use of non-orthogonal quantum states, while remaining simple enough for use in an undergraduate educational setting.

The reduced complexity of the B92 protocol compared to BB84 arises from the use of only two states instead of four, resulting in fewer detectors and simpler state preparation. This not only simplifies the experimental setup but also emphasizes the inherent efficiency of the B92 protocol for secure quantum communication

3.1. Introducing Eve

In real-world scenarios, the security of quantum communication is often compromised by an eavesdropper (Eve). Eve attempts to intercept the quantum channel between Alice and Bob to gain information about the key. However, the fundamental principles of quantum mechanics, including the no-cloning theorem and the disturbance caused by measurement, make eavesdropping detectable.

3.2. Eve's Interaction with the Quantum Channel

If Eve intercepts the quantum state sent from Alice to Bob, she must choose the basis on which to measure the quantum state. Given that the states used in the B92 protocol are non-orthogonal, Eve's selection introduces an unavoidable uncertainty:

- If Eve measures in the **+ basis** or **x basis**, the quantum state collapses, meaning Bob may receive a state that is different from what Alice originally sent.
- If Bob's basis does not match Eve's chosen basis, the quantum measurement statistics will reveal discrepancies between Alice's and Bob's results.

3.3. Detection of Eve's Presence

The presence of Eve can be detected by comparing a subset of the granted bits that Alice and Bob have kept. If Eve measures the quantum state, her actions cause errors in Bob's measurements. This leads to a deviation from the expected proportion of "granted" bits, thereby indicating the presence of eavesdropping.

3.4. Experimental Perspective with Eve

In an experimental implementation, the quantum channel can be monitored for error rates. The presence of an eavesdropper will introduce a higher-than-expected error rate in the bits Bob receives and ultimately grants. By comparing a subset of the final key over a classical public channel, Alice and Bob can estimate the error rate and detect the presence of an eavesdropper.

4. Theory of Experiment

4.1. One-Time Pad

The one-time pad [24,25] is a classical encryption technique assisted by quantum physics to meet the method's requirements and is considered 100% secure in principle. While the desired message consists of a non-random sequence of 0 s and 1 s, the one-time pad is a single-use key consisting of a random sequence of 0 s and 1 s. A binary addition [26,27] of the message to the key results in another sequence of random bits, which is then sent as the encrypted message.

The addition rules for the bits are:

$$0+0=0; \quad 1+0=1; \quad 0+1=1; \quad 1+1=0. \tag{1}$$

When applying a binary addition with the secure key generated by the B92 protocol to the original message, the sender can encrypt the message. By applying a binary addition with the secure key to the encrypted message, the receiver can decrypt it and obtain the original message. An example is shown in Table 1.

Table 1. XOR Encryption and Decryption of Letters M, I, and T.

Letter	Definition	Binary Value	Key (8-bit)	XOR Result
M	ASCII Decrypted	01001101 01001101	11010011	10011110
I	ASCII Decrypted	01001001 01001001	01101110	00100111
T	ASCII Decrypted	01010100 01010100	10100101	11110001

If the encrypted message is intercepted, the eavesdropper requires the key to decode the message, otherwise the random sequence cannot be interpreted. The binary sequence can be converted to strings using the American Standard Code for Information Interchange (ASCII) [28]. An example of the one-time pad is shown in Table 1.

While computer-generated pseudo-random numbers are not truly (100%) random [29], the one-time pad requires a completely random selection of the encryption key. Nonetheless, quantum physics offers numerous possibilities for true randomness [30], such as radioactive decay. Quantum random number generators are a key component of quantum cryptography data networks. In practice, a photon that is reflected by a beam-splitter can be interpreted as 1 and a photon that is transmitted by a beam-splitter can be interpreted as 0.

Therefore, in a conventional light source with the same intensity [31,32], photon distribution on two single photo-detectors can be considered truly random.

Generally, the B92 protocol's core purpose is to generate a secure key between the sender and the receiver.

4.2. Key Distribution

The sending unit 'Alice' consists of a pulsed laser source [31,32], which is polarized in a specific direction, and a half-wave plate ($\lambda/2$ with λ being the wavelength), which rotates the polarization of the incident light by doubling the physical rotation angle of the plate. We note that the mentioned angle refers to the rotation angle of the polarization and not of the plate.

The receiving unit 'Bob' consists of a beam-splitter, a half-wave plate ($\lambda/2$), a polarizing beam-splitters (PBS) and two two detectors to indicate whether the light sent by Alice was reflected or transmitted through the PBS.

A schematic sketch of Alice and Bob is provided in Figure 1.

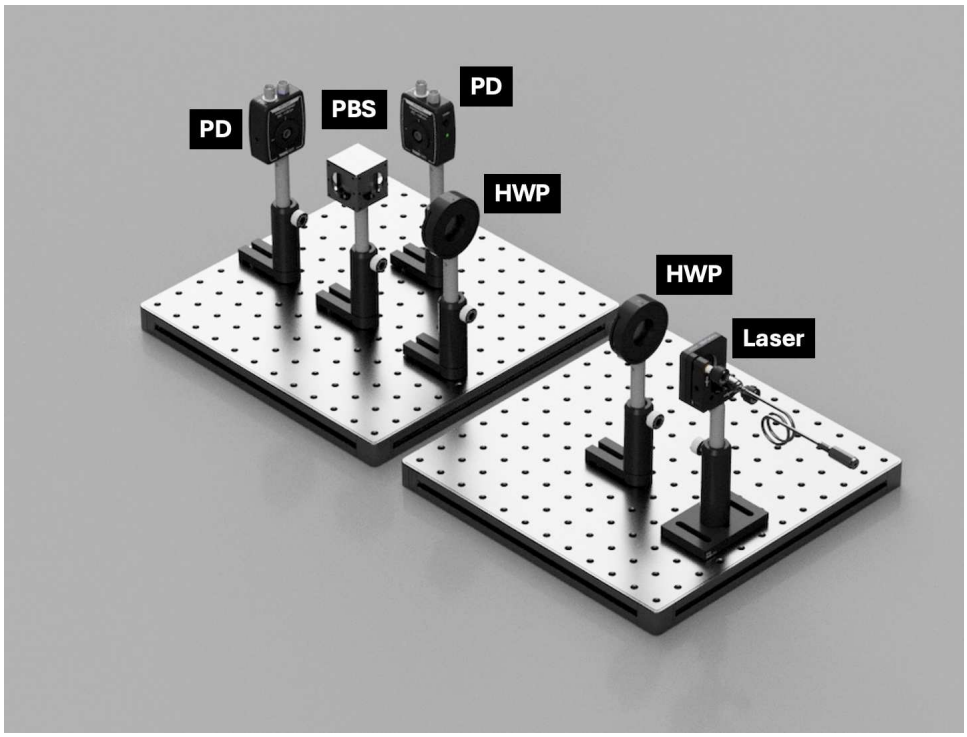

Figure 1. Optical diagram with the bases + (0° and 90°) and x (−45° and 45°). The (**right**) breadboard represents Alice's unit, while the (**left**) breadboard corresponds to Bob's unit. "PBS" defines the polarizing beam-splitter. "PD" defines the photodiode. "HWP" defines the half wave plate.

A secure key must be generated before Alice can send a message to Bob. If Alice's pulsed source is polarized horizontally, two bases can be defined, "+" and "x", where each contains two light polarizations. Alice can send a random bit of 0 or 1 in both bases. The "+" basis consists of 0° and 90° polarizations, while the "x" basis consists of −45° and 45° polarizations. In general, either basis can be used to represent a binary bit: "0' for 90° and −45° and "1' for 0° and 45°.

In the B92 algorithm, we limit Alice's options to two choices: a state of "1" in the "x" basis (which corresponds to 45°) and a state of "0" in the "+" basis (which corresponds to 0°).

To create a secure key, Alice randomly selects a bit and adjusts the polarization plate accordingly, which also determines the basis for the bit. After making her selection, she sends the bit to Bob using the scheme described above.

Bob randomly selects a basis, determining which of the two detectors he uses for measurement—either the detector without a half-wave plate ("+" basis) or the detector with a half-wave plate ("x" basis). He then records which detector registered the bit.

If Alice sends "0" in the "x" basis and Bob measures in the same "x" basis, he will always measure "0". However, if he measures in the "+" basis, he has a 50% chance to measure "0" and a 50% to measure "1". We note that the Thorlabs EDU-QCRY1 system employs a random bit selection mechanism when the intensity at the two photodiodes (PD) is equal. This approach ensures that the protocol's behavior remains consistent with the theoretical model. In our implementation, we adopt a similar method for handling cases where the encoding and measurement basis do not correspond, as detailed in the experimental setup section. This occurs because the polarizing beam splitter (PBS) transmits light polarized at 0° degrees and reflects light polarized at 90° degrees.

In the B92 protocol, not all transmitted bits are accepted as part of the final key. Some bits are discarded since we cannot be 100% certain of their original value, as explained earlier. The accepted bits, known as 'impossible bits,' are those where Bob receives a bit that we know Alice could not have sent due to the restrictions placed on her choices. These impossible bits are: "1" in the "+" basis (corresponding to 90°) and "0" in the "x" basis (corresponding to -45°).

By testing all possible combinations of Alice's transmissions and Bob's measurements, it becomes clear that only one transmission option from Alice can result in Bob receiving these bits. When Bob measures these bits, he can be 100% sure that he has received exactly what Alice sent. After each measurement, Bob announces whether the bit was accepted or denied via the public channel.

The encryption key is derived only from the accepted measurements. For a complete list of transmission options. see Table 2.

If there is no eavesdropper, the probability of accepting a single bit is 25%. A detailed explanation of this calculation will be provided in Section 4.4.

4.3. Detection of an Eavesdropper

The eavesdropper unit 'Eve' is positioned between Alice and Bob, as shown in Figure 3. Eve's setup consists of the same components, but in reverse order. It is strategically placed to measure the light coming from Alice and then transmit the same information to Bob.

As Eve cannot copy the pulsed beam transmitted by Alice without altering its state, she must randomly select the basis on which it will be transmitted to Bob. In addition, a random basis must be selected for the bit received from Alice. Therefore, two random selections are required for Eve's bases. Alice and Bob continue their protocol as they would without Eve. However, due to Eve's interference, there are now instances wherein a bit is accepted, but it is not the original bit that Alice sent. For all transmission options, see Figure 4.

With the eavesdropper present, Bob accepts 37.5% of the bits. Eve is detected because this acceptance rate is 12.5% higher than expected. A detailed explanation of this calculation will be provided in Section 4.4.

Table 2. Quantum cryptographic encoding and decoding of letters M, I, and T using random bitwise keys for secure message transmission.

Message					**M**			
Binary Message	0	1	0	0	1	1	0	1
+								
Random Key	1	1	0	1	0	0	1	1
Encrypted Message	1	0	0	1	1	1	1	0
+								
Random Key	1	1	0	1	0	0	1	1
Decrypted Message	0	1	0	0	1	1	0	1
Message					M			
Message					**I**			
Binary Message	0	1	0	0	1	0	0	1
+								
Random Key	0	1	1	0	1	1	1	0
Encrypted Message	0	0	1	0	0	1	1	1
+								
Random Key	0	1	1	0	1	1	1	0
Decrypted Message	0	1	0	0	1	0	0	1
Message					I			
Message					**T**			
Binary Message	0	1	0	1	0	1	0	0
+								
Random Key	1	0	1	0	0	1	0	1
Encrypted Message	1	1	1	1	0	0	0	1
+								
Random Key	1	0	1	0	0	1	0	1
Decrypted Message	0	1	0	1	0	1	0	0
Message					T			

4.4. Mathematical Description in Dirac Notation

The four polarization states in this experiment are $|-45^\circ\rangle$, $|0^\circ\rangle$, $|45^\circ\rangle$, $|90^\circ\rangle$, where $|0^\circ\rangle, |90^\circ\rangle$ are the states of the "+" basis and $|-45^\circ\rangle, |45^\circ\rangle$are the states of the "x" basis. They are defined using Dirac's bra-ket notation [33], where $|v\rangle$ denotes a vector that represents a quantum state, and $\langle f|$ denotes a linear map that maps a vector to a number in the complex plane.

Consequently, the linear functional acting on a vector is written as $\langle f|v\rangle$, corresponding to a scalar product for two states [34,35]. The scalar product of two orthogonal states is: $\langle 90^\circ|0^\circ\rangle = 0$, whereas the squared absolute value of the scalar product represents the probability that a 0° polarized pulsed beam passes through a polarizer oriented in a 90°direction. The scalar product of the same two states is: $\langle 0^\circ|0^\circ\rangle = 1$.

These states can be expressed as linear combinations of the other basis, $|\psi\rangle = \alpha|\phi_1\rangle + \beta|\phi_2\rangle$. Since the scalar product must be normalized, $\langle\psi|\psi\rangle = 1$, all four states can be expressed by a superposition of the others:

$$|45^\circ\rangle = \frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle,$$

$$|-45^\circ\rangle = \frac{1}{\sqrt{2}}|0^\circ\rangle - \frac{1}{\sqrt{2}}|90^\circ\rangle,$$

$$|0^\circ\rangle = \frac{1}{\sqrt{2}}|45^\circ\rangle + \frac{1}{\sqrt{2}}|-45^\circ\rangle,$$

$$|90^\circ\rangle = \frac{1}{\sqrt{2}}|45^\circ\rangle - \frac{1}{\sqrt{2}}|-45^\circ\rangle.$$

Thus, for example, the probability of a 0° polarized pulsed beam passing a 45° oriented polarizer is 50%:

$$|\langle 45^\circ|0^\circ\rangle|^2 = |\frac{1}{\sqrt{2}}\langle 45^\circ|45^\circ\rangle + \frac{1}{\sqrt{2}}\langle 45^\circ|-45^\circ\rangle|^2 = \frac{1}{2}$$

The probability for the other states and bases can be derived similarly.

Here, we re-derive the projections of the measurement operators $\hat{M}$ for both possible and impossible bits in the context of eavesdropping in the B92 protocol. Specifically, we examine the projections for the possible bits at angles 0° and 45° and for the impossible bits at 90° and -45°, which could result from an eavesdropper (Eve).

The base operators, which are linear maps that input a ket $|v_1\rangle$ and output a ket $|v_2\rangle$, are introduced to describe a measurement in either of the bases.

$$\hat{M}_+ = |0^\circ\rangle\langle 0^\circ| - |90^\circ\rangle\langle 90^\circ|, \tag{2}$$

$$\hat{M}_x = |45^\circ\rangle\langle 45^\circ| - |-45^\circ\rangle\langle -45^\circ|. \tag{3}$$

The operators act on a given state, and when an operator acts on a basis that matches the polarized state, the eigenvalue corresponds to the state itself. Note that an eigenvalue of -1 corresponds to transmission and is assigned as bit 0.

For example:

$$\hat{M}_+|0^\circ\rangle = |0^\circ\rangle\langle 0^\circ|0^\circ\rangle - |90^\circ\rangle\langle 90^\circ|0^\circ\rangle = |0^\circ\rangle$$
$$\hat{M}_+|90^\circ\rangle = |0^\circ\rangle\langle 0^\circ|90^\circ\rangle - |90^\circ\rangle\langle 90^\circ|90^\circ\rangle = -|90^\circ\rangle.$$

The same can be derived for $\hat{M}_x$ operating on the x base. However, if an operator acts on the opposite basis, it is possible to show that the transmission probability of a pulsed beam through a polarizer is 50%:

$$\hat{M}_+|45^\circ\rangle = |0^\circ\rangle\langle 0^\circ|45^\circ\rangle - |90^\circ\rangle\langle 90^\circ|45^\circ\rangle =$$
$$|0^\circ\rangle\langle 0^\circ|(\frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle) - |90^\circ\rangle\langle 90^\circ|(\frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle) =$$
$$\frac{1}{\sqrt{2}}|0^\circ\rangle - \frac{1}{\sqrt{2}}|90^\circ\rangle. \tag{4}$$

Similarly, for the other cases:

$$\hat{M}_+|-45^\circ\rangle = \frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle, \tag{5}$$

$$\hat{M}_x|0^\circ\rangle = \frac{1}{\sqrt{2}}|45^\circ\rangle - \frac{1}{\sqrt{2}}|-45^\circ\rangle, \tag{6}$$

$$\hat{M}_x|90^\circ\rangle = \frac{1}{\sqrt{2}}|45^\circ\rangle + \frac{1}{\sqrt{2}}|-45^\circ\rangle. \quad (7)$$

By re-analyzing the projections on the basis states associated with $\hat{M}_+$ (for 0° and 90° bases) and $\hat{M}_x$ (for 45° and −45° bases), we can quantify the probability distributions and detection rates that serve as eavesdropping indicators. This derivation provides insight into how each of Eve's basis choices affects the measured statistics and how the expected and observed rates of impossible bits compare.

Figures 2 and 4 show different cases for Alice and Bob with and without an eavesdropper.

Alice			**Bob**			
State	Basis	Bit	Basis	State	Measured Bit	Approval
$\|0^\circ\rangle$	+	0	+	$\hat{M}_+\|0^\circ\rangle = \|0^\circ\rangle$	$\|0^\circ\rangle = 0$	Denied
			×	$\hat{M}_x\|0^\circ\rangle = \frac{1}{\sqrt{2}}\|45^\circ\rangle - \frac{1}{\sqrt{2}}\|-45^\circ\rangle$	$\|45^\circ\rangle = 1$	Denied
					$\|-45^\circ\rangle = 0$	Granted
$\|45^\circ\rangle$	×	1	+	$\hat{M}_+\|45^\circ\rangle = \frac{1}{\sqrt{2}}\|0^\circ\rangle - \frac{1}{\sqrt{2}}\|90^\circ\rangle$	$\|0^\circ\rangle = 0$	Denied
					$\|90^\circ\rangle = 1$	Granted
			×	$\hat{M}_\times\|45^\circ\rangle = \|45^\circ\rangle$	$\|45^\circ\rangle = 1$	Denied

Bob approved: Bit can be used
Measurement is discarded

Figure 2. Alice and Bob basis, bits and measured bit without Eve.

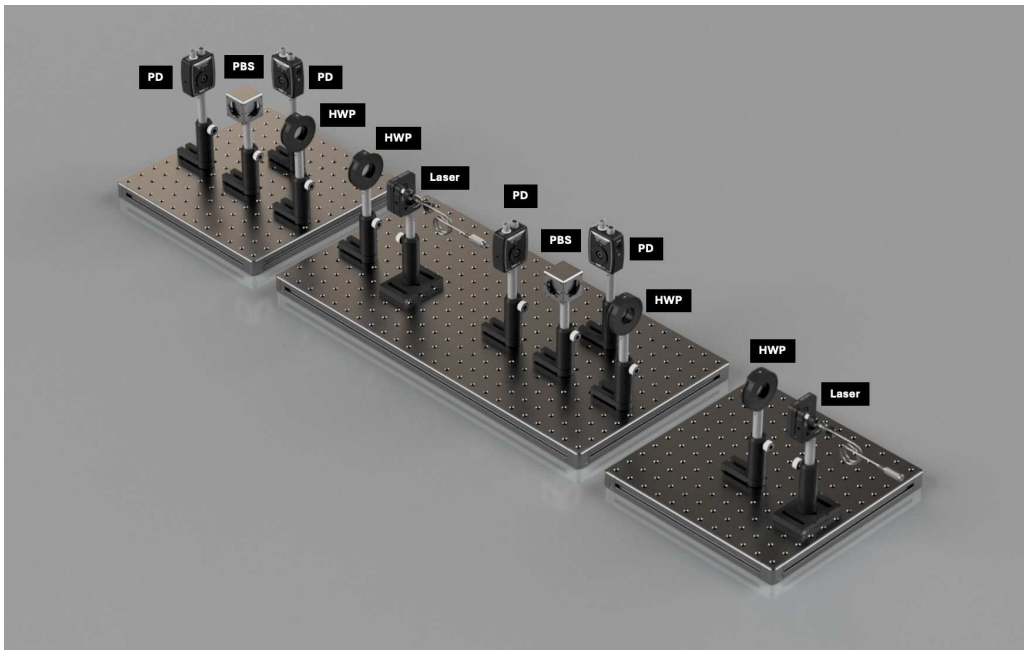

Figure 3. Optical diagram with the bases + (0° and 90°) and x (−45° and 45°). The (**left**) breadboard represents Bob's unit, the (**middle**) section corresponds to Eve's interception point, and the (**right**) breadboard represents Alice's unit. "PBS" defines the polarizing beam-splitter. "PD" defines the photodiode. "HWP" defines the half wave plate.

Alice			Eve			Bob			
State	Basis	Bit	Basis	State	State Sent	Basis	State	Bit Measured	Approval
$\|0^\circ\rangle$	+	0	+	$\hat{M}_+\|0^\circ\rangle = \|0^\circ\rangle$	$\|0^\circ\rangle$	+	$\hat{M}_+\|0^\circ\rangle = \|0^\circ\rangle$	$\|0^\circ\rangle = 0$	Denied
						×	$\hat{M}_\times\|0^\circ\rangle = \frac{1}{\sqrt{2}}\|45^\circ\rangle - \frac{1}{\sqrt{2}}\|-45^\circ\rangle$	$\|45^\circ\rangle = 1$	Denied
								$\|-45^\circ\rangle = 0$	Granted
			×	$\hat{M}_\times\|0^\circ\rangle = \frac{1}{\sqrt{2}}\|45^\circ\rangle - \frac{1}{\sqrt{2}}\|-45^\circ\rangle$	$\|45^\circ\rangle$	+	$\hat{M}_+\|45^\circ\rangle = \frac{1}{\sqrt{2}}\|0^\circ\rangle - \frac{1}{\sqrt{2}}\|90^\circ\rangle$	$\|0^\circ\rangle = 0$	Denied
								$\|90^\circ\rangle = 1$	Granted
						×	$\hat{M}_\times\|45^\circ\rangle = \|45^\circ\rangle$	$\|45^\circ\rangle = 1$	Denied
					$\|-45^\circ\rangle$	+	$\hat{M}_+\|-45^\circ\rangle = \frac{1}{\sqrt{2}}\|0^\circ\rangle + \frac{1}{\sqrt{2}}\|90^\circ\rangle$	$\|0^\circ\rangle = 0$	Denied
								$\|90^\circ\rangle = 1$	Granted
						×	$\hat{M}_\times\|-45^\circ\rangle = -\|-45^\circ\rangle$	$\|-45^\circ\rangle = 0$	Granted
$\|45^\circ\rangle$	×	1	+	$\hat{M}_+\|45^\circ\rangle = \frac{1}{\sqrt{2}}\|0^\circ\rangle - \frac{1}{\sqrt{2}}\|90^\circ\rangle$	$\|0^\circ\rangle$	+	$\hat{M}_+\|0^\circ\rangle = \|0^\circ\rangle$	$\|0^\circ\rangle = 0$	Denied
						×	$\hat{M}_\times\|0^\circ\rangle = \frac{1}{\sqrt{2}}\|45^\circ\rangle - \frac{1}{\sqrt{2}}\|-45^\circ\rangle$	$\|45^\circ\rangle = 1$	Denied
								$\|-45^\circ\rangle = 0$	Granted
					$\|90^\circ\rangle$	+	$\hat{M}_+\|90^\circ\rangle = -\|90^\circ\rangle$	$\|90^\circ\rangle = 1$	Granted
						×	$\hat{M}_\times\|90^\circ\rangle = \frac{1}{\sqrt{2}}\|45^\circ\rangle + \frac{1}{\sqrt{2}}\|-45^\circ\rangle$	$\|45^\circ\rangle = 1$	Denied
								$\|-45^\circ\rangle = 0$	Granted
			×	$\hat{M}_\times\|45^\circ\rangle = \|45^\circ\rangle$	$\|45^\circ\rangle$	+	$\hat{M}_+\|45^\circ\rangle = \frac{1}{\sqrt{2}}\|0^\circ\rangle - \frac{1}{\sqrt{2}}\|90^\circ\rangle$	$\|0^\circ\rangle = 0$	Denied
								$\|90^\circ\rangle = 1$	Granted
						×	$\hat{M}_\times\|45^\circ\rangle = \|45^\circ\rangle$	$\|45^\circ\rangle = 1$	Denied

Bob approved: Bit can be used
Measurement is discarded

Figure 4. Alice and Bob Basis, Bits and measured Bit with Eve.

5. Experimental Procedure

The light source in the experimental system is a pulsed laser rather than a single-photon source, meaning that full prevention of interception cannot be guaranteed. Therefore, to eavesdrop, Eve must separate a portion of the light transmitted from Alice, analyze part of it, and send the remainder to Bob without detection. However, the sequence of the protocol in this experiment is identical to that of a true quantum encryption system. To avoid biased randomization, all bases and bits for Alice, Bob, and Eve should be generated simultaneously. The complete experimental setup is shown in Figure 3.

5.1. Calibration

The lasers in the system are the CPS635R (Thorlabs) model [36]; collimated laser diode module: 635 nm, 1.2 mW, Gaussian profile beam. The detector models are EDU-QCRY1/M by Thorlabs. It is worth noting that the CPS635R-C2 laser module used in our experiment operates a pulse width on the order of nanoseconds. In contrast, the bit rate in our experiment is approximately one bit per second, meaning that each laser pulse is significantly shorter than the time interval between successive bits. This ensures that the optical signal remains well-defined and easily detectable.

These properties of the pulsed laser are particularly relevant for educational demonstrations, as they enable a clear distinction between individual transmission events, allowing students to analyze quantum measurement principles effectively. This setup also emulates single-photon transmission scenarios while remaining cost-effective and practical for laboratory use.

Before conducting the experiment, the light source and the detectors were calibrated [31,32]. The pulsed laser was calibrated by a polarizer to a horizontal polarization of 90°. Both Bob's and Eve's detectors were aligned so that transmitted and reflected light would reach the desirable detector. Both detectors were also tested for each base and bit.

5.2. Key Transmission Without Eve

Alice randomly chooses a bit (0 or 1) while Bob randomly selects his basis (+ or x), as illustrated in Figure 2. Alice adjusts her wave plate accordingly, and Bob determines which sensor pair he will use to receive the signal. The random selection of bases and bits is made

using a computational script, which is explained later in the paper. The laser pulse is then sent through the setup, and Bob records whether he measured a 0 or 1 bit, along with the chosen basis. He then transmits, via the public channel, whether he accepted or denied the bit. At the end of the process, the bits accepted by Bob form the shared encryption key. Using this key, Alice can encrypt the message and send it to Bob. Bob can then decrypt the message using the same key.

5.3. Key Transmission with Eve

The complete key distribution process in the B92 protocol can be described through a series of steps illustrating how information is prepared, transmitted, and measured, and how potential eavesdropping can be detected.

Briefly, Alice randomly selects a bit (0 or 1) and prepares a photon polarized at one of two non-orthogonal states. Bob randomly selects a measurement basis (+ or x) to detect the photon, while Eve, as an eavesdropper, intercepts and retransmits the photon using randomly chosen bases. If the bases are mismatched, inconsistencies arise in Bob's measurements, enabling the detection of eavesdropping, as illustrated in Figure 4. Below are the detailed steps the protocol involves:

Step 1: The pulsed laser is set to one of two non-orthogonal polarization angles. For example, Alice prepares a state polarized at 45°, representing one of the two non-orthogonal states used in the B92 protocol.

Step 2: Alice sends the prepared state using the pulsed laser, emulating a single-photon state. The specific state to be sent is chosen randomly. For example, Alice may send the state representing "1" (polarized at 45°).

Step 3: Eve intercepts the photon, chooses a random basis, and measures the state by projecting it along one of the two non-orthogonal states used by Alice. If Eve's chosen basis matches Alice's polarization state (i.e., Eve chooses 45° in our example), she will measure the state with high certainty. Otherwise, the result is probabilistic. Let us assume that in our example, Eve indeed chooses 45°, thus successfully measuring the state.

Step 4: If Eve successfully measures the state, she records the result as "1" and prepares a new state to send to Bob. In the B92 protocol, one state (e.g., 45°) corresponds to a successful detection, representing a "1" bit, while the other state (e.g., 0°) ideally results in no detection, effectively indicating the absence of an encoded bit. However, if Eve's measurement basis does not match Alice's transmitted state, she may still obtain a result, but it will be probabilistic and can be projected into a different state. Consequently, the bit Eve retransmits could differ from Alice's original bit, leading to inconsistencies in Bob's measurements. These inconsistencies manifest as detectable errors, signaling the presence of eavesdropping. In our example, let us assume that Eve successfully measures "1" and retransmits it.

Step 5: Eve prepares the transmitted photon with the same polarization she measured and sends a new laser pulse, emulating the single-photon state detected from Alice.

Step 6: Bob chooses a random measurement basis. In the B92 protocol, Bob uses a detector corresponding to one of the two non-orthogonal states. In our example, let us assume that Bob chooses the same basis as Alice (i.e., 45°). Thus, he successfully detects the photon and records the bit as "1."

Step 7: If Bob's measurement basis matches Alice's original state, he successfully detects the pulse and records the correct bit ("1") with certainty. If Bob's basis does not match Alice's original state, the result is probabilistic, introducing the chance of an incorrect detection due to the nature of non-matching basis measurements.

Step 8: Alice continues the process by sending subsequent bits, repeating the steps for each bit in her message.

These steps are repeated for all subsequent bits in the key distribution process, with each bit undergoing the same sequence of preparation, transmission, measurement, and eavesdropping detection to ensure the security and integrity of the protocol. The error bars in the experimental data were estimated by considering both statistical and systematic uncertainties.

5.4. Quantum Bit Error Rate (QBER)

The quantum bit error rate (QBER) is a key metric used to quantify the performance and security of a quantum key distribution (QKD) system. It is defined as the ratio of erroneous bits received by Bob to the total number of bits transmitted by Alice, expressed as a percentage. The QBER is given by [37]

$$\text{QBER} = \frac{N_{\text{error}}}{N_{\text{total}}} \times 100\%, \tag{8}$$

where N_{error} is the number of bits received by Bob that do not match Alice's transmitted bits, and N_{total} is the total number of bits transmitted by Alice. The QBER reflects the error rate in the communication channel and can indicate the presence of an eavesdropper, as errors introduced by Eve's interference cause the QBER to rise above its expected baseline. In our experiments, we calculate the QBER for different scenarios (with and without eavesdropping) to evaluate the reliability of the B92 protocol implementation and to demonstrate how disturbances in the quantum channel are detected through variations in the QBER. This metric serves as a crucial indicator of the protocol's integrity and security.

6. Computational Procedure

For the B92 protocol, MATLAB (MathWorks, Natick, Massachusetts, USA, version, MATLAB R2024b) scripts were meticulously developed to serve as a digital twin of the experimental setup, offering an accessible and comprehensive platform to explore the protocol's key principles and security features. These simulations focused on two primary cases: one involving only Alice and Bob and another incorporating an eavesdropper, Eve, between Alice and Bob. The digital twin enables a detailed analysis of the convergence of granted bit rates, providing a critical bridge between theoretical expectations and simulated outcomes.

In the first case, the simulation models the ideal scenario where only Alice and Bob interact, with Bob measuring the bits transmitted by Alice according to their respective measurement bases. This highlights the foundational mechanics of the protocol. The second case introduces Eve, who intercepts and measures Alice's bits before retransmitting them to Bob. This scenario showcases the probabilistic interference caused by Eve's actions, manifesting in increased bit error rates and altered convergence behavior.

Both cases were simulated in a series of increasing bit sample sizes, defined by the following values:

$$N_{\text{values}} = [20, 50, 100, 200, 400, 800, 1600, 5000, 20000, 40000] \tag{9}$$

The results showed convergence toward the expected granted bit rates: approximately 25% in the Alice–Bob configuration, indicating successful bit retention in the absence of an eavesdropper, and around 37.5% in the Alice–Eve–Bob configuration, reflecting the additional errors introduced by Eve's interference.

On a single core of an Intel Xeon E5-2697v2 CPU, the average running time for each of these simulations over the chosen N_{values} was 26 s. In contrast, running the simulations on an M4 Pro achieved a significantly faster average runtime of 1.15 s. A comparison of

the average simulation run time on various CPUs is shown in Table 3. This efficient performance, especially on modern processors, underscores the feasibility of using MATLAB for large-scale simulations of quantum key distribution protocols, enabling practical analysis of convergence behavior in B92 under realistic computational constraints.

Table 3. Average run times of simulations on various CPUs.

CPU Type	Average Run Time (Seconds)
Apple M4 Pro	1.15
AMD Ryzen 7 7840U	2.75
Apple M2	3.85
Intel Core i7-12700H	6.35
Intel Xeon E5-2697v2	26.00

This approach effectively illustrates the theoretical foundations of the B92 protocol and its sensitivity to eavesdropping, as evidenced by the measurable increase in granted bits when Eve is active in the communication channel. By faithfully replicating the experimental conditions in a computational environment, this simulation—serving as a digital twin of the experiment—empowers students and researchers in resource-constrained settings to engage with quantum cryptography without requiring expensive physical setups. Additionally, the simulation code for the B92 protocol, which serves as a critical resource for replicating these experiments, is publicly available on GitHub [38].

7. Results

Tables summarizing the results for each part, including the randomly generated bases and bits, are given in Appendix A.

7.1. Alice and Bob Without Eve

First, we generated 45 and 100 random bits by selecting two non-orthogonal bases. This was achieved through two nested loops: one to determine the bit value and another to select the basis. To generate $|0\rangle$, we used the bit value '0' with the '+' basis, whereas for generating $|1\rangle$, the bit value '1' was combined with the 'x' basis. This process was implemented using the initial stage of the experimental setup, with Alice being the first isle in Figure 1.

Subsequently, Bob, the second isle in Figure 1, generated a random sequence of 45 bases, which he used in conjunction with his two detectors to measure the incoming bits from Alice. Bob retained only the "impossible bits", defined as instances where the measurement outcomes could not align with Alice's original bit values due to the protocol's design. Specifically, these impossible bits occur when Alice transmits $|0\rangle$ and Bob measures $|1\rangle$ in the '+' basis, or when Alice transmits $|1\rangle$ and Bob measures $|0\rangle$ in the 'x' basis.

It is important to note that these impossible bits correspond to specific polarization states: the bit value '1' in the '+' basis, associated with 90°, and the bit value '0' in the 'x' basis, associated with $-45°$. This distinction plays a critical role in the security of the B92 protocol, as the detection of such bits allows Bob to identify key bits with absolute certainty, assuming no eavesdropping occurs. The procedure highlights the reliance on quantum mechanical principles, particularly the disturbance induced by measurements, to ensure secure communication.

7.2. Alice and Bob with Eve

In this case, Eve is introduced into the communication channel between Alice and Bob, as depicted in Figure 3, where it occupies the middle isle of the experimental setup. Eve intercepts and measures the quantum states sent by Alice and then retransmits the

measured states to Bob, while attempting to remain undetected. This interception introduces disturbances into the communication channel due to the fundamental principles of quantum mechanics, which ensure that measurements of non-orthogonal quantum states cannot be performed without altering their original properties.

In our experiment, we monitor Eve's presence by analyzing the proportion of "granted" bits—the subset of bits retained by Bob after matching his measurement basis with the transmitted state. This proportion is then compared against the expected theoretical values derived from the protocol. As illustrated in Figure 5, the deviation in the proportion of "granted" bits serves as an indicator of Eve's interference. In a secure, undisturbed channel between Alice and Bob, the proportion of "granted" bits stabilizes around 25%. However, when Eve is introduced, this value rises to approximately 37.5%, as summarized in Table 4.

The increase in the "granted" bit proportion is a direct consequence of Eve's interference. The experimental data shows (as shown in Table 5) that when Eve intercepts a quantum state, she must choose a basis for measurement. If her chosen basis matches Alice's transmitted basis, Eve can measure the state with high accuracy and retransmit it to Bob. However, if her basis does not match Alice's, Eve's measurement collapses the quantum state into a new one, deviating from Alice's original encoding. Evidently, this probabilistic disturbance is propagated to Bob, who may receive altered states that do not align with the original protocol design. Consequently, we observe that this disruption changes the statistical probabilities of Bob's measurements, increasing the likelihood of granting bits that deviate from the expected pattern in direct Alice-Bob communication.

Table 4. Proportion of "granted" bits for two simulation runs: one with 45 bits and one with 100 bits. Results are shown for both Alice and Bob without Eve and Alice with Eve and Bob.

	Experiment 1 (45 bits)	**Experiment 2 (100 bits)**
Alice + Bob	30.0%	26.0%
Alice + Eve + Bob	37.9%	37.5%

Table 5. Summary of quantum bit error rate (QBER) calculations for experiments with and without eavesdropping. Errors are calculated as the deviation of granted bits from the expected value based on Alice and Bob's ideal communication (25% granted bits). QBER is calculated as the percentage of errors relative to the total bits sent.

Experiment	**Bits Sent**	**Granted Bits (%)**	**Granted Bits**	**Errors**	**QBER (%)**
Alice + Bob (Exp 1)	45	30.0	13.5	2.25	5.0
Alice + Eve + Bob (Exp 1)	45	37.9	17.1	5.9	12.9
Alice + Bob (Exp 2)	100	26.0	26.0	1.0	1.0
Alice + Eve + Bob (Exp 2)	100	37.5	37.5	12.5	12.5

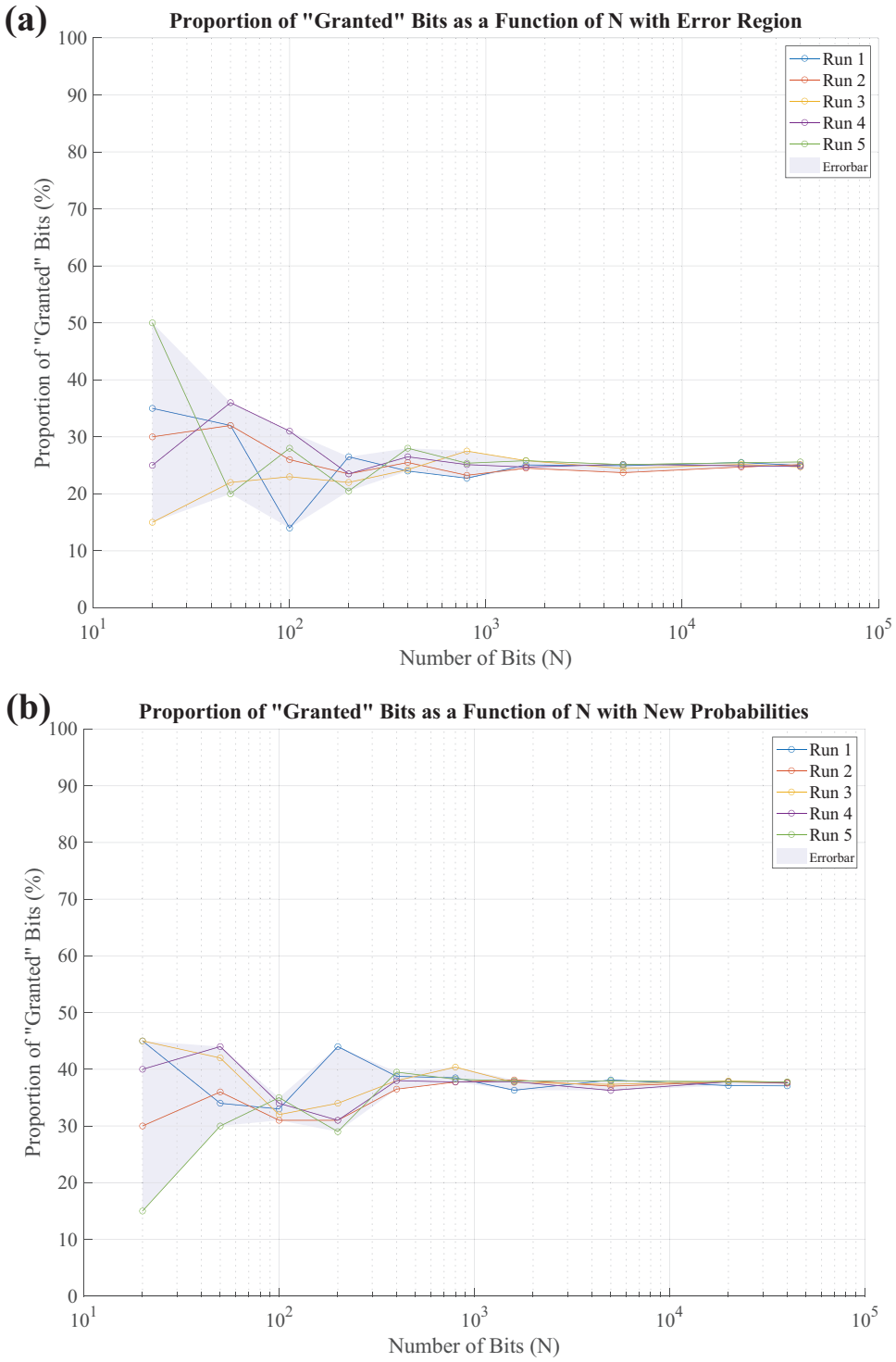

Figure 5. Simulation results for the proportion of "granted" bits as a function of the number of transmitted bits N. The runs correspond to the values $N = [20, 50, 100, 200, 400, 800, 1600, 5000, 20{,}000, 40{,}000]$, showcasing convergence behavior. Error bars represent the variability across different runs, with the expected granted bit rate approximating 25% for the Alice–Bob setup (**a**) and 37.5% for the Alice–Eve–Bob setup due to errors introduced by the eavesdropper (**b**).

8. Discussion

The experiment presented here effectively showcases the principles of the B92 quantum cryptography protocol, offering an educational and accessible framework for exploring fundamental QKD concepts. By employing classical optical components such as pulsed lasers and polarizers, the setup avoids reliance on costly single-photon sources, significantly

reducing the barriers to being implemented by institutions and individuals interested in quantum cryptography. This practical approach not only enables hands-on exploration of the B92 protocol but also bridges the gap between theoretical quantum mechanics and its real-world applications. The experimental results closely align with theoretical predictions, demonstrating the protocol's robustness in detecting eavesdropping through observable deviations in granted bit rates.

The B92 protocol's reliance on just two non-orthogonal quantum states and a pair of detectors highlights its simplicity and effectiveness for educational and experimental applications. This minimalistic design not only simplifies experimental setups, making it ideal for introductory quantum communication courses and workshops but also demonstrates the protocol's inherent efficiency as a practical introduction to secure quantum communications. Compared to BB84, the most commonly used QKD protocol, B92 requires a less complex experimental setup, utilizing only two detectors and a single pulsed laser source. In contrast, BB84 employs four distinct quantum states and multiple detectors to account for all possible measurement outcomes, increasing alignment complexity and equipment demands. While BB84 enables detection across a broader range of states, the simple design of B92 significantly reduces technical and financial demands, making it particularly suitable for institutions focused on illustrating the foundational principles of QKD. We note that the B92 protocol offers several advantages compared to other QKD protocols, particularly BB84. Its simplicity, requiring only two non-orthogonal states instead of four, reduces the complexity of state preparation and minimizes the number of required detectors. This makes B92 more accessible for educational implementations and lowers hardware costs. Additionally, its security is based on the fundamental principle that an eavesdropper cannot perfectly distinguish non-orthogonal states without introducing errors. Unlike BB84, which requires a more complex state preparation and detection scheme, B92 simplifies the hardware requirements while still maintaining a high level of security. The protocol's reliance on non-orthogonal states ensures that any measurement by an eavesdropper introduces detectable disturbances, making it inherently secure against standard intercept-resend attacks. While B92's key generation rate is lower due to post-selection, its efficiency can be enhanced through optimized detection schemes and integration with advanced signal processing techniques. Free-space QKD is a growing field, particularly in applications such as satellite-based quantum communication, drone-to-ground secure links, and long-range atmospheric quantum key distribution. In free-space QKD, photons must traverse an open-air medium rather than a guided optical fiber, introducing unique challenges such as atmospheric turbulence, beam divergence, and background noise from sunlight or city lights. B92, like BB84 and other free-space QKD protocols, must be evaluated in terms of its resilience to these challenges and its adaptability for real-world implementations. One of the main challenges in free-space QKD is the attenuation and distortion of the optical beam due to atmospheric effects, such as turbulence, scattering, and absorption. These effects can lead to fluctuations in photon arrival times and polarization distortions. For polarization-based protocols like B92 and BB84, atmospheric turbulence can alter the polarization state of transmitted photons, potentially reducing key generation rates. However, adaptive optics and real-time polarization compensation techniques can mitigate these issues. B92's simplicity, requiring only two non-orthogonal states instead of four, reduces the complexity of real-time polarization tracking compared to BB84, potentially making it easier to implement in long-range free-space channels. In contrast, time-bin and phase-encoded free-space QKD protocols are inherently less sensitive to turbulence since they do not rely on maintaining a stable polarization state. However, these protocols require more sophisticated phase stabilization techniques, which add to the system's complexity. A major advantage of free-space QKD is the potential for long-distance quantum communication,

including satellite-to-ground and drone-based QKD links. One of the key security concerns in free-space QKD is the risk of intercept-resend attacks, where an eavesdropper (Eve) attempts to measure and retransmit quantum states without detection. Since B92 relies on non-orthogonal states, it offers strong security against direct intercept-resend attacks, as Eve cannot measure the transmitted quantum states without introducing detectable errors. However, in free-space implementations, an attacker might attempt beam-splitting attacks, where a portion of the transmitted beam is siphoned off without fully disturbing the remaining signal. To counter such attacks, decoy-state techniques can be integrated into B92, ensuring that the key distribution remains secure even in free-space environments. Another potential security enhancement is post-selected quantum state filtering, whereby Alice and Bob discard bits that show signs of eavesdropping-induced perturbations, increasing the protocol's robustness against side-channel attacks. Future improvements to B92 for free-space QKD could include hybrid implementations combining B92 with phase-based or entanglement-assisted QKD techniques. Additionally, leveraging emerging integrated photonics technology could enable miniaturized B92 systems suitable for spaceborne and mobile quantum communication platforms. While BB84 and other free-space QKD protocols have been widely implemented in real-world systems, B92 provides an alternative with reduced hardware complexity, simplified state preparation, and strong security against measurement-based eavesdropping attacks. By optimizing its implementation through wavelength selection, temporal filtering, and hybrid encoding techniques, B92 has the potential to be a valuable protocol for secure, high-performance quantum communication in free-space applications.

An important aspect of eavesdropping in the B92 protocol is the unambiguous state discrimination (USD) attack, which represents one of the most effective strategies for this protocol. In a USD attack, Eve can deterministically identify Alice's state in certain cases without introducing errors, as described by the referee. For example, if Alice sends $|0\rangle$ and Eve measures $|-45\rangle$, she can conclusively determine that Alice sent $|0\rangle$. Eve's optimal strategy in such cases is to retransmit $|0\rangle$ and discard all other results. While this approach allows Eve to obtain an exact copy of Alice's and Bob's sifted strings, it reduces the fraction of the sifted key rather than introducing additional QBER. This is a relevant topic that could be demonstrated using our educational setup, offering students deeper insights into the vulnerabilities of the B92 protocol and the nuances of quantum eavesdropping strategies.

Although the current implementation emphasizes the B92 protocol, this experiment provides a versatile foundation that can be expanded in several ways. One potential use is the inclusion of additional QKD protocols, such as the Differential Phase Shift (DPS) protocol [39]. The DPS protocol, introduced in 2002, uses the relative phase difference between consecutive coherent light pulses to encode key information [40]. Including the DPS protocol in the experimental setup would enable the exploration of a phase-based QKD scheme, contrasting it with the prepare-and-measure approach of B92. This comparison would improve our understanding of different encoding mechanisms, security features, and the practical considerations of implementing phase-coherent protocols.

Incorporating the DPS protocol could also inspire discussions about its practical applications, particularly its suitability for long-distance QKD in optical fiber networks [41]. The DPS protocol's robustness against photon-number-splitting (PNS) attacks and its compatibility with coherent light sources make it a strong candidate for scalable and efficient implementations. A hybrid experimental setup combining the non-orthogonal state preparation of B92 with the relative phase encoding of DPS could further enrich the learning experience. Such a setup would provide insight into multiprotocol systems designed for specific challenges, such as high-loss environments or metropolitan QKD networks [42,43].

In real-world contexts, the DPS protocol's advantages make it a compelling addition. Its efficient use of coherent pulses and relative phase encoding aligns with the practical requirements of fiber-based quantum networks, offering robustness and simplicity for deployment in large-scale infrastructure. Adapting the experimental setup to include DPS-like capabilities would highlight these practical aspects, further emphasizing the relevance of QKD protocols in addressing contemporary cyber-security challenges [44]. One of the key advantages of our experimental setup is its affordability compared to single-photon-based QKD systems. Our setup, which relies on a pulsed laser source and standard optical components, has an estimated cost of approximately USD 3000. In contrast, an experiment using true single-photon sources requires significantly more expensive equipment. For example, a correlated photon source such as the SPDC810N costs USD 25,500, and each single-photon detector module costs around USD 4916. Since at least two detectors are required, the total cost exceeds USD 50,000, more than ten times the cost of our proposed setup. For educational purposes, it is worth mentioning that B92 and BB84 protocols are not intrinsically quantum-enhanced, as they do not rely on features like entanglement or N00N states. However, these protocols remain valuable for teaching the basics of quantum key distribution. Additionally, techniques like decoy states could address no-cloning loopholes, offering further potential for future educational developments.

The presented experiment serves as both an accessible introduction to quantum cryptography principles and a scalable platform for advanced research and practical applications. Its modular design and adaptability enable future enhancements, such as integrating phase modulators, quantum random number generators, or additional detection systems, transforming it into a fully functional QKD system capable of supporting various protocols [45]. This flexibility not only ensures its continued relevance for educational and research purposes but also highlights its potential to inspire innovations in low-cost, high-security communication systems, positioning it as a cornerstone for advancements in quantum cryptography.

We conclude that the methodology outlined in this paper extends beyond the realm of optics, finding applications in diverse areas of physics in which hydrodynamics systems serve as analogs for quantum mechanical matter wave dynamics [46]. This approach reinforces the broader framework of quantum-classical analogies, offering new perspectives for understanding fundamental quantum phenomena through accessible classical systems [47–50]. By establishing a foundational link between these disciplines, this work contributes a crucial building block to the development of intuitive and pedagogically effective quantum-inspired classical experiments.

Author Contributions: Conceptualization, supervision, software, and methodology, G.G.R.; Software, validation, formal analysis, investigation, writing, S.P.G.; Project administration, review, and editing, A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The simulations mentioned in this article are available online [38]. Experimental data are available in the supplementary material.

Acknowledgments: We thank Haim Suchowski, Shimshon Bar-Ad, and the School of Physics and Astronomy at Tel Aviv University for providing us with the necessary tools and laboratory equipment to carry out this study. We extend our gratitude to Ady Arie for his invaluable guidance, wisdom, and unwavering support.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Raw Data

Table A1. Alice and Bob's Basis and Bit Values for 45 bits.

Alice Basis	Alice Bit	Bob Basis	Bob Bit
x	1	+	0
x	1	x	1
x	1	x	1
x	1	x	1
x	1	+	0
x	1	+	1
+	0	+	0
+	0	+	0
+	0	+	0
x	1	+	1
x	1	+	0
x	1	x	1
x	1	x	1
+	0	x	1
+	0	x	1
+	0	x	1
+	0	+	0
+	0	+	0
x	1	+	0
+	0	x	0
x	1	+	0
x	1	+	1
+	0	+	0
+	0	x	0
x	1	x	1
+	0	+	0
x	1	+	0
x	1	+	1
+	0	x	0
+	0	x	1
+	0	+	0
x	1	+	1
+	0	x	1
x	1	x	1
+	0	+	0
+	0	+	0
x	1	+	1
x	1	+	1
x	1	x	1
+	0	+	0
+	0	+	0
+	0	x	1
x	1	+	1
x	1	+	0
+	0	x	0

Table A2. Alice and Bob's Basis and Bit Values for the Extended Dataset.

Alice Basis	Alice Bit	Bob Basis	Bob Bit
x	0	x	0
x	1	x	1
+	1	+	1
+	0	+	1
x	0	x	0
+	1	x	1
x	1	+	1
+	1	+	1
x	1	x	1
+	1	+	1
x	1	+	0
+	1	x	0
x	1	+	0
+	1	+	1
x	0	+	0
+	0	x	1
+	0	+	0
+	1	+	1
+	0	+	0
x	0	+	0
+	1	+	1
+	1	x	0
+	0	+	0
x	0	+	0
+	1	+	1
+	0	x	1
+	1	+	1
x	1	x	1
+	0	+	0
+	1	x	0
x	0	+	0
+	1	x	0
x	0	x	0
x	1	x	1
x	1	x	1
x	0	x	0
x	0	x	0
+	0	x	1
x	0	x	0
+	0	+	0
x	1	x	1
x	0	x	0
+	1	+	1
+	0	+	0
x	0	+	0
+	1	+	1
x	0	x	0
x	1	x	1
+	1	+	1
x	1	x	1
+	1	x	0
+	0	+	0
+	1	+	1
x	1	x	1
x	1	+	1
+	0	+	0

Table A2. *Cont.*

Alice Basis	Alice Bit	Bob Basis	Bob Bit
x	1	x	1
x	1	+	0
x	1	x	1
x	1	x	1
+	1	+	1
x	0	x	0
+	0	x	1
x	1	x	1
+	0	x	1
+	1	+	1
+	1	+	1
+	1	x	0
+	0	+	1
+	0	x	1
x	1	x	1
x	0	+	1
+	0	+	0
+	1	+	1
+	1	x	0
x	1	+	0
x	1	x	1
x	0	+	0
+	0	x	0
x	0	+	1
x	1	x	1
x	0	+	1
x	1	x	1
+	0	+	0
x	0	+	0
x	0	+	0
x	1	+	0
+	0	+	0
+	1	+	1
+	0	x	0
x	1	+	0
+	1	+	1
x	0	+	0
+	1	x	0
+	0	x	0
x	0	+	1
x	0	x	0
x	0	x	0
+	1	+	1
+	1	x	0

Table A3. Alice, Eve, and Bob's Basis and Bit Values for 45 bits.

Alice Basis	Alice Bit	Eve Incident Basis	Eve Basis Transmitted	Bob Basis	Bob Bit
+	0	x	x	+	1
+	1	x	+	x	0
+	0	x	x	x	1
+	0	x	x	x	1

Table A3. *Cont.*

Alice Basis	Alice Bit	Eve Incident Basis	Eve Basis Transmitted	Bob Basis	Bob Bit
x	0	+	x	x	1
+	0	x	x	x	1
x	0	+	x	x	0
x	0	+	x	x	1
+	0	+	x	x	0
x	1	x	x	x	1
x	0	x	x	x	1
x	1	+	x	x	1
+	1	+	+	+	1
+	0	+	+	+	0
x	0	+	x	x	1
+	0	+	x	x	0
x	1	x	x	x	1
x	0	+	+	+	1
x	1	x	+	+	1
+	1	+	x	x	0
+	0	+	+	+	1
x	1	x	x	+	0
x	1	x	x	+	0
+	0	x	+	+	1
+	0	+	+	+	0
+	0	x	x	x	1
x	0	+	+	+	1
+	1	x	+	x	1
x	0	+	+	x	1
x	1	+	+	+	1
x	1	x	+	+	1
+	0	+	+	+	0
x	1	x	x	+	0
+	1	+	x	+	0
x	1	x	+	+	1
+	1	x	+	+	1
+	0	x	x	+	0
+	1	+	+	+	1
+	1	+	x	+	1
+	0	x	+	x	1
+	0	+	+	+	0
+	1	x	+	+	1
+	0	x	x	x	1
+	0	+	+	x	0
x	1	+	+	x	1
+	1	+	x	x	1
x	0	+	x	+	0

Table A4. Alice, Eve, and Bob's Basis and Bit Values for 100 bits.

Alice Basis	Alice Bit	Eve Incident Basis	Eve Basis Transmitted	Bob Basis	Bob Bit
0	+	1	x	0	x
0	+	0	+	0	+
0	+	0	x	0	x
0	+	1	x	0	+
0	+	1	x	1	x

Table A4. *Cont.*

Alice Basis	Alice Bit	Eve Incident Basis	Eve Basis Transmitted	Bob Basis	Bob Bit
1	x	0	+	1	x
1	x	1	x	1	+
1	x	1	x	1	+
0	+	0	x	0	x
0	+	0	+	0	x
0	+	0	+	0	+
0	+	1	x	0	+
1	x	1	x	1	x
0	+	0	x	0	x
0	+	1	x	0	+
1	x	0	+	1	+
1	x	1	x	1	x
1	x	0	+	0	+
0	+	0	+	0	+
1	x	1	x	1	+
1	x	0	+	1	+
0	+	0	+	1	x
0	+	0	x	1	x
1	x	1	+	1	x
0	+	0	+	1	x
0	+	1	x	0	+
1	x	0	+	1	x
1	x	0	+	1	x
1	x	1	x	1	+
0	+	0	x	0	+
1	x	1	x	0	+
1	x	1	x	1	+
1	x	1	+	1	+
1	x	0	+	0	+
1	x	0	+	1	+
0	+	0	x	0	+
0	+	0	+	0	+
0	+	0	x	0	+
0	+	0	+	1	x
0	+	0	x	0	x
1	x	0	+	1	+
0	+	0	+	0	+
0	+	0	x	0	x
1	x	1	x	1	+
0	+	1	x	0	x
0	+	0	+	0	x
1	x	1	x	1	+
0	+	0	+	0	+
0	+	0	x	0	+
1	x	1	x	1	+
0	+	0	+	0	x
0	+	1	x	0	+
1	x	0	+	0	+
0	+	1	x	0	+
0	+	0	x	1	x
1	x	0	+	0	+
1	x	1	x	1	x
0	+	0	+	1	x

Table A4. *Cont.*

Alice Basis	Alice Bit	Eve Incident Basis	Eve Basis Transmitted	Bob Basis	Bob Bit
0	+	0	x	1	x
0	+	1	x	0	x
1	x	1	+	0	+
0	+	0	+	1	x
1	x	1	+	1	x
1	x	0	+	0	+
0	+	0	x	1	x
1	x	1	x	0	+
0	+	0	x	0	+
0	+	0	x	0	x
1	x	1	x	1	+
1	x	1	x	0	+
0	+	1	x	0	+
1	x	1	x	1	x
1	x	0	+	0	+
1	x	0	+	1	+
0	+	1	x	0	+
1	x	1	x	1	+
0	+	0	x	0	+
1	x	1	x	1	x
0	+	0	+	0	+
1	x	1	+	1	x
1	x	1	x	1	+
1	x	0	+	1	+
1	x	1	+	1	x
0	+	1	x	0	x
1	x	1	x	1	+
1	x	0	+	1	x
1	x	1	+	0	+
0	+	0	+	0	+
0	+	0	x	1	x
0	+	1	x	0	x
1	x	1	x	1	+
0	+	0	x	0	+
0	+	0	+	0	+
1	x	1	x	0	+
1	x	1	x	1	x
0	+	0	+	0	x
0	+	1	x	0	x
0	+	0	+	1	x
1	x	0	+	1	x
1	x	1	x	1	+

References

1. Williamson, S.M.; Prybutok, V. Balancing privacy and progress: A review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Appl. Sci.* **2024**, *14*, 675. [CrossRef]
2. Xu, F.; Ma, X.; Zhang, Q.; Lo H.K.; Pan, J.W. Quantum cryptography with realistic devices. *arXiv* **2019**, arXiv:1903.09051.
3. Liao, S.K.; Yong, H.L.; Liu, C.; Shentu, G.L.; Li, D.D.; Lin, J.; Dai, H.; Zhao, S.Q.; Li, B.; Guan, J.Y.; et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nat. Photonics* **2017**, *11*, 509–513. [CrossRef]
4. Rozenman, G.G.; Kundu, N.K.; Liu, R.; Zhang, L.; Maslennikov, A.; Reches, Y.; Youm, H.Y. The quantum internet: A synergy of quantum information technologies and 6G networks. *IET Quantum Commun.* **2023**, *4*, 147–166. [CrossRef]
5. Bennett, C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121. [CrossRef]
6. Charles, H.; Bennett, G.B.; Ekert, A.K. Quantum cryptography. *Sci. Am.* **1992**, *267*, 50–57.

7. Waldvogel, C.P.; Massey, J.L. The probability distribution of the Diffie-Hellman key. In *International Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1992.
8. Ladd, T.D.; Jelezko, F.; Laflamme, R.; Nakamura, Y.; Monroe, C.; O'Brien, J.L. Quantum computers. *Nature* **2010**, *464*, 45–53. [CrossRef]
9. Hassija, V.; Chamola, V.; Goyal, A.; Kanhere, S.S.; Guizani, N. Forthcoming applications of quantum computing: Peeking into the future. *IET Quantum Commun.* **2020**, *1*, 35–41. [CrossRef]
10. Blinder, S.M. *Introduction to Quantum Mechanics*; Academic Press: London, UK, 2020.
11. Begimbayeva, Y.; Zhaxalykov, T. Research of quantum key distribution protocols: BB84, B92, E91. *Sci. J. Astana IT Univ.* **2022**. [CrossRef]
12. Iqbal, H.; Krawec, W.O. Analysis of a high-dimensional extended B92 protocol. *Quantum Inf. Process.* **2021**, *20*, 1–22. [CrossRef]
13. Tudorache, A.G.; Manta, V.; Caraiman, S. Quantum steganography based on the B92 quantum protocol. *Mathematics* **2022**, *10*, 2870. [CrossRef]
14. Dutta, A.; Muskan; Banerjee, S.; Pathak, A. Analysis for Satellite-Based High-Dimensional Extended B92 and High-Dimensional BB84 Quantum Key Distribution. *Adv. Quantum Technol.* **2024**, *7*, 2400149. [CrossRef]
15. García-Beltrán, G.; Mercado-Zúñiga, C.; René Torres-SanMiguel, C.; Gallegos-García, G.; Torres-Torres, C. Photonic encryption by optical activity in Kerr-like carbon-based nanofluids with plasmonic nanoparticles. *J. Mol. Liq.* **2022**, *367*, 120424. [CrossRef]
16. Rahmanpour, M.; Erfanian, A.; Afifi, A.; Khaje, M.; Hossein Fahimifar, M. A new quantum key distribution protocol to reduce afterpulse and dark counts effects. *Results Opt.* **2024**, *16*, 100718. [CrossRef]
17. Bloom, Y.; Fields, I.; Maslennikov, A.; Rozenman, G.G. Quantum cryptography—A simplified undergraduate experiment and simulation. *Physics* **2022**, *4*, 104–123. [CrossRef]
18. Rozenman, G.G.; Peisakhov, A.; Zadok, N. Dispersion of organic exciton polaritons—A novel undergraduate experiment. *Eur. J. Phys.* **2022**, *43*, 035301. [CrossRef]
19. Griffiths, B.J. Cryptography in undergraduate education: Perceptions of postgraduate students. *Cryptologia* **2021**, *45*, 553–562. [CrossRef]
20. Asfaw, A.; Blais, A.; Brown, K.R.; Celaria, J.; Cantwell, C.; Carr, L.D.; Combes, J.; Debroy, D.M.; Donohue, J.M.; Economou, S.E.; et al. Building a quantum engineering undergraduate program. *IEEE Trans. Educ.* **2022**, *65*, 220–242. [CrossRef]
21. Dzurak, A.S.; Epps, J.; Laucht, A.; Malaney, R.; Morello, A.; Nurdin, H.I.; Pla, J.J.; Saraiva, A.; Yang, C.H. Development of an undergraduate quantum engineering degree. *IEEE Trans. Quantum Eng.* **2022**, *3*, 1–10. [CrossRef]
22. Uehara, G.; Larson, J.; Barnard, W.; Esposito, M.; Posta, F.; Yarter, M.; Sharma, A.; Kyriacou, N.; Dobson, M.; Spanias, A. Undergraduate research and education in quantum machine learning. In Proceedings of the 2022 IEEE Frontiers in Education Conference (FIE), Uppsala, Sweden, 8–11 October 2022.
23. Lethen, T. Bit commitment as an introduction to quantum cryptography. *Eur. J. Phys.* **2022**, *43*, 055402. [CrossRef]
24. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
25. Bellovin, S.M. Frank Miller: Inventor of the one time pad. *Cryptologia* **2011**, *35*, 203–222. [CrossRef]
26. Bender, A.; Beller, S. Mangarevan invention of binary steps for easier calculation. *Proc. Natl. Acad. Sci. USA* **2014**, *111*, 1322–1327. [CrossRef] [PubMed]
27. Chrisomalis, S. *Numerical Notation: A Comparative History*; Cambridge University Press: Cambridge, UK, 2010. [CrossRef]
28. Mackenzie, C.E. *Coded Character Sets, History and Development*; Addison-Wesley Pub.: Boston, MA, USA, 1979.
29. Barker, E.; Kelsey, J. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*; Technical Report; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2015. [CrossRef]
30. Bird, J.J.; Ekert, A.; Faria, D.R. On the effects of pseudorandom and quantum-random number generators in soft computing. *Soft Comput.* **2020**, *24*, 9243–9256. [CrossRef]
31. Born, M.; Wolf, E. *Principles of Optics*, 7th ed.; Cambridge University Press: Cambridge, UK, 2002. [CrossRef]
32. Fowles, G.R. *Introduction to Modern Optics*, 2nd ed.; Dover Publications: Mineola, NY, USA, 1989.
33. Shankar, R. *Principles of Quantum Mechanics*; Springer Science & Business Media: New York, NY, USA, 2012.
34. Griffiths, D.J.; Schroeter, D.F. *Introduction to Quantum Mechanics*; Cambridge University Press: Cambridge, UK, 2018. [CrossRef]
35. Muller-Kirsten, H.J.W. *Introduction to Quantum Mechanics: Schrodinger Equation and Path Integral*; World Scientific Co., Ltd.: Hoboken, NJ, USA, 2012. [CrossRef]
36. ThorLabs. Laser Modules: 635 nm. 2022. Available online: https://www.thorlabs.com/thorproduct.cfm?partnumber=CPS635 (accessed on 27 February 2025).
37. Kollmitzer, C.; Pivk, M. *Applied Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2010. [CrossRef]
38. Gandelman, S.P.; Maslennikov, A; Rozenman G.G. Hands-On Quantum Cryptography: Undergraduate Experimentation with the B92 Protocol, 2024. Available online: https://github.com/Sara-Gandelman/Hands-On-Quantum-Cryptography-Undergraduate-Experimentation-with-the-B92-Protocol (accessed on 27 February 2025).

39. Gu, J.; Cao, X.Y.; Yin, H.L.; Chen, Z.B. Differential phase shift quantum secret sharing using a twin field. *Opt. Express* **2021**, *29*, 9165–9173. [CrossRef]
40. Akihiro Mizutani, Y.T.; Tamaki, K. Finite-key security analysis of differential-phase-shift quantum key distribution. *Phys. Rev. Res.* **2023**, *5*, 023132. [CrossRef]
41. Zhang, Y.; Chen, Z.; Pirola, S.; Wang, X.; Zhou, C.; Chu, B.; Zhao, Y.; Xu, B.; Yu, S.; Guo, H. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.* **2020**, *125*, 010502. [CrossRef] [PubMed]
42. Chen, T.Y.; Jiang, X.; Tang, S.B.; Zhou, L.; Yuan, X.; Zhou, H.; Wang, J.; Liu, Y.; Chen, L.K.; Liu, W.Y.; et al. Implementation of a 46-node quantum metropolitan area network. *NPJ Quantum Inf.* **2021**, *7*, 134. [CrossRef]
43. Kržič, A.; Sharma, S.; Spiess, C.; Chrashekara, U.; Töpfer, S.; Sauer, G.; del Campo González-Martín, L.J.; Kopf, T.; Petscharnig, S.; Grafenauer, T.; et al. Towards metropolitan free-space quantum networks. *NPJ Quantum Inf.* **2023**, *9*, 95. [CrossRef]
44. Sharikov, P. Contemporary cybersecurity challenges. In *The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network*; Springer International Publishing: Cham, Switzerland, 2023; pp. 143–157.
45. Liu, R.; Rozenman, G.G.; Kundu, N.K.; Chandra, D.; De, D. Towards the industrialisation of quantum key distribution in communication networks: A short survey. *IET Quantum Commun.* **2022**, *3*, 151–163. [CrossRef]
46. Rodrigues Gonçalves, M.; Rozenman, G.G.; Zimmermann, M.; Efremov, M.A.; Case, W.B.; Arie, A.; Shemer, L.; Schleich, W.P. Bright and dark diffractive focusing. *Appl. Phys. B* **2022**, *128*, 51. [CrossRef]
47. Rozenman, G.G.; Bondar, D.I.; Schleich, W.P.; Shemer, L.; Arie, A. Observation of Bohm trajectories and quantum potentials of classical waves. *Phys. Scr.* **2023**, *98*, 044004. [CrossRef]
48. Rozenman, G.G.; Ullinger, F.; Zimmermann, M.; Efremov, M.A.; Shemer, L.; Schleich, W.P.; Arie, A. Observation of a phase space horizon with surface gravity water waves. *Commun. Phys.* **2024**, *7*, 165. [CrossRef]
49. Weisman, D.; Carmesin, C.M.; Rozenman, G.G.; Efremov, M.A.; Shemer, L.; Schleich, W.P.; Arie, A. Diffractive guiding of waves by a periodic array of slits. *Phys. Rev. Lett.* **2021**, *127*, 014303. [CrossRef] [PubMed]
50. Rozenman, G.G.; Bondar, D.I.; Schleich, W.P.; Shemer, L.; Arie, A. Bohmian mechanics of the three-slit experiment in the linear potential. *Eur. Phys. J. Spec. Top.* **2023**, *232*, 3295–3301. [CrossRef]